

F-Secure VPN+:

PKI Integration with Netscape Certificate Management System

F-Secure Corporation Securing the Mobile Distributed Enterprise

F-Secure VPN+: PKI Integration with Netscape Certificate Management System

Implementation Guide, October 2000

All product names referenced herein are trademarks or registered trademarks of their respective companies. F-Secure[™] Corporation disclaims proprietary interest in the marks and names of others. Although F-Secure Corporation makes every effort to ensure that this information is accurate, F-Secure Corporation will not be liable for any errors or omission of facts contained herein. F-Secure Corporation reserves the right to modify specifications cited in this document without prior notice.

Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of F-Secure Corporation.

The purpose of this document is to help you identify the strengths of the integrated security solutions the F-Secure product line provides. It is not a comparative review of competitor's products but it may provide valuable information that will assist you see what makes our offering different from all the others.

USA	Europe
F-Secure Inc.	F-Secure Corporation
675 N. First Street, 5 th floor	PL 24
San Jose, CA 95112, USA	FIN-02231 Espoo, Finland
Tel (408) 938 6700	Tel +358 9 859 900
Fax (408) 938 6701	Fax +358 9 8599 0599
http://www.F-Secure.com/	http://www.F-Secure.com/

Copyright © 1995-2000 F-Secure Corporation. All rights reserved.

Contents

1	Exec	utive Summary	1		
2	Requ	irements	1		
3	B Assumptions				
4	Insta	lling PKI System	2		
	4.1	Install Netscape Certificate Management System 4.2	2		
	4.2	Run CMS Installation Wizard	9		
	4.3	Configure SCEP Enrolment	26		
5	Integ	ration with F-Secure VPN+	31		
	5.1	Add CA Certificate as Trusted Root	31		
	5.1	.1 Export CA Certificate	31		
	5.1	.2 Import CA Certificate as Trusted Root	31		
	4.1	Configure Certificate Handling	32		
	4.1	.1 Enable SCEP Enrollment	32		
	4.1	.2 Enable CRL Retrieval	33		
	4.2	Create Connection Template	33		
	5.2	Known Issues	39		

1 Executive Summary

F-Secure VPN+ is a software-based virtual private network that provides total end-to-end security by protecting every link in the corporate network chain including clients, servers, and gateways.

F-Secure VPN+ integrates with our world-class distributed firewall, anti-virus, and desktop encryption solutions under one policy management system, enabling you to deploy and manage your crucial security applications throughout the world from a single location and maintain complete transparency to the end-user.

F-Secure VPN+ supports SCEP and LDAP protocols for automated certificate enrollment, revocation, and updating, eliminating the need to manually download certificates and Certificate Revocation Lists (CRLs). F-Secure VPN+ has been tested and proven to interoperate with Netscape Certificate Management System. This implementation guide will detail the necessary steps to configure and use F-Secure VPN+ with Netscape Certificate Management System.

2 Requirements

Before you begin, you should have access to the following:

- □ NT Server with Service Pack 6a or later
- Netscape Certificate Management System 4.2 installation media An evaluation version of this software can be downloaded from <u>http://www.iPlanet.com</u>.

3 Assumptions

The following assumptions have been made for the purposes of this document. If these assumptions are not correct for your individual installation, some of the information contained here may be inapplicable or incorrect.

- □ All of the PKI components (LDAP Server and CA) will be residing on the same physical server. Minor adjustments will need to be made to the installation procedures if some or all of these components are placed on separate servers.
- None of components have been installed on the server yet. It may only be necessary to make configuration changes instead of performing a complete installation of some components.
- Server components (e.g. LDAP) will be used only for the PKI system. If this is not the case, additional installation options may be required.

□ **This PKI System is being set up for demonstration purposes only.** In the case of a production system additional steps must be taken to enhance security.

4 Installing PKI System

4.1 Install Netscape Certificate Management System 4.2

Run Setup.exe from Netscape Certificate Management System 4.2 installation media.



Click Next at the Welcome screen.



Click Yes to accept the License Agreement.

F-SECURE CORPORATION



Select "Netscape Servers" as the type of setup and click Next.

Select Installation Type		
	Choose the typ	e of Setup you prefer, then click Next.
	C <u>E</u> xpress	Products will be installed with the most common options. Recommended for novice users and those who wish to evaluate the software.
SS - S	• Typical	Products will be installed with some of the more common options. Recommended for intermediate users who wish to quickly install.
×	O C <u>u</u> stom	You may choose all of the options you want to install, and provide detailed configuration information. Recommended for advanced users.
		< Back Next > Cancel

Select "Typical" setup type and click Next.

Choose Installation Directory		
	Setup will install Netscape Server Products in the following directory. This directory will be referred to as the "Installation directory" or the "Server Root."	
AD	To install to this directory, click Next. To install to a different directory, click Browse and select another directory.	
Ŷ	You can choose not to proceed with installation by clicking Cancel to exit Setup.	
	Installation Directory C:\Netscape\Server4 Browse	
	< <u>B</u> ack <u>N</u> ext > Cancel	

Click *Next* to accept the default directory of C:\Netscape\Server4.

Select Products		
	Select the products you want to install, clear the product do not want to install.	ducts you
	Products:	
	✓ Netscape Server Products Core Components	18 MB
The -	Netscape Directory Suite	19 MB
LAN	Administration Services	19 MB
	Vetscape Certificate Management System	86 MB
	Netscape Directory Server 4.1 Synch Service	OK
¥,	Description Core Server Components used by Char Netscape Server Products	inge
	Space Required: 145 MB Space Available: 15	582 MB
	< <u>B</u> ack <u>N</u> ext >	Cancel

Select all components except the "Netscape Directory Server 4.1 Synch Service". Click *Next*.

Directory Server 4.1	Netscape server information is stored in the Netscape configuration directory server, which you may have already set up. If so, you should configure this server to be managed by the configuration server. Configuration Directory Server This instance will be the configuration directory server Use existing configuration directory server Host: Port: 389 Bind As: admin Password:	×
	< <u>B</u> ack <u>N</u> ext > Cancel	

Select the option to make this server the configuration directory server and click Next.

Directory Server 4.1		×
	You may already have a directory server you want to use to store your data, such as user and group information. Directory to store data Store data in this directory server Store data in an existing directory server Host: Port: 389 Bind As: cn=Directory Manager Password: Suffix: p=f-secure.com	
	< <u>B</u> ack <u>N</u> ext > Can	cel

Select the option to store data in this directory server and click Next.

Directory Server 4.1 S	Settings this directory server will use for basic operation. General Settings Server Identifier: fsca Server Port: 389 Suffix: o=f-secure.com
	< <u>B</u> ack <u>Next</u> Cancel

Enter the directory server settings and click Next.

Server Identifier: host name of certificate server Server Port: 389 Suffix: o=<domain name>

Directory Server 4.1 N	etscape configuration directory server administrator	×
	The Netscape configuration directory administrator is the ID typically used to log in to the console. Configuration Directory Server Administrator Configuration Directory Administrator Configuration Directory Administrator Administrator ID: Password: reserver Password (again):	
	< Back Next> Cance	

Enter the administrator ID and password and click Next.

Directory Server 4.1 A	dministration Domain × The Administration Domain is a part of the configuration directory server used to store information about Netscape software. If you are managing multiple software releases at the same time, or managing information about multiple domains, you may use the the Administration Domain to keep them separate. If you are not using administrative domains, select the default. Otherwise, enter a descriptive, unique name for the administration domain, such as the name of the organization responsible for managing the domain.
	Administration f-secure.com Domain: < <u>B</u> ack <u>Next></u> Cancel

Enter the domain name or some other unique identifier as the "Administration Domain" and click *Next*.

Directory Server 4.1 D	irectory Manager Settings
	Certain directory server operations require an administrative user. This user is referred to as the Directory Manager and typically has a bind Distinguished Name (DN) of cn=Directory Manager. The password for the Directory Manager must be at least 8 characters long. Directory Manager Settings Directory Manager DN: cn=Directory Manager Password: xxxxxxx Password (again): xxxxxxx
< <u>B</u> ack <u>Next></u> Cancel	

Enter the "Directory Manager DN" and password, then click Next.

Administration Server I	Port Selection
	The Administration Server runs on a different network port from other servers on this system. This port number determines how it can be accessed. A random port number has been chosen below.
	Administration Port: 1657
	You can access this server by clicking on the Netscape Console icon in the Netscape Server Family program group.
¥	http://fsca.f-secure.com:1657/
	By default, this Administration Server will run using the System Account. This setting can be changed through the Services Control Panel or through the administration interface.
	< Back Next > Cancel

Accept the randomly generated administration port unless you require it to run on a specific port and click *Next*.

Netscape Certificate M	anagement System 4.2 Server Identifier	×
	Each instance of the Netscape Certificate Management System requires a unique identifier. Press Enter to accept the default, or type in another name and press Enter. Netscape Certificate Management System Settings Server Identifier:	
	< <u>B</u> ack <u>Next></u> Cancel	

Click *Next* to accept the "Server Identifier" which is set to the server host name by default.

Configuration Summary	
	Setup has gathered the information to perform the installation. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files. Current Settings: [Netscape Server Products] Installation Directory/Server Root: C:\Netscape\Server4 [Server Core Binaries] [Netscape Server Products Core Components] [Netscape Server Products Core Components] [Netscape Server Products Common files] [Core Java classes] [Java Runtime Environment] [Netscape Server Products Common files]
	< <u>B</u> ack <u>Next></u> Cancel

Click Next to begin copying files.



When the installation has finished, choose to "Restart my computer now" and click *Finish*.

4.2 Run CMS Installation Wizard

Start the Netscape Console from Start – Programs – Netscape Server Products – Netscape Console 4.2.

.NI Netscape Console			
User ID:	admin		
Password:	******		
Administration URL:	http://fsca.f-secure.com:1657	•	
ОК	Cancel Help		

Log in as admin with the password you specified during the above installation.



Browse to the instance of CMS in the console window and click the *Open* button. This will start the CMS Installation Wizard.

IN Installation Wizard	×
[Introduction	
This installation wizard will take you through the steps of setting up the Netscape Certificate Management System (CMS).	
<back next=""> Cancel</back>	Help

Click Next at the Introduction screen.

N Installation Wizard		X
Internal Database Specify the LDAP serve used to store requests a	er to use for the CMS internal database. This internal database is and certificate records.	
Instance ID:	fsca-db	
Port number:	38900	
Directory manager DN:	cn=Directory Manager	
Password:	*****	
Password (again):	******	
	<back next=""> Cancel Help</back>	

F-SECURE CORPORATION

Enter the password for the cn=Directory Manager user and confirm it. Click Next.

Installation Wiza				
Administrator				
	the privileged user who car nd password for the CMS a		window. Specif	y the
Administrator ID:	admin			
Full name:	Certificate Management S	ystem Administra	tor	
Password:	*****			
Password (again):	*****			
	<back< td=""><td>Next> 0</td><td>Cancel</td><td>Help</td></back<>	Next> 0	Cancel	Help

Enter a password for the CMS administrator user and click Next.

C F-Secure Corporation

12

N Installation Wizard	×
Subsystems	
Select the subsystems to be installed:	
C Certificate Manager	
O Registration Manager	
Data Recovery Manager	
<back next=""> Cancel</back>	Help

Select to install the "Certificate Manager" subsystem with no Data Recovery Manager and click *Next*.

Installation Wizard	
Remote Data Recovery Mana	ger
Do you want to connect the	current subsystems to a remote data recovery manager?
No	
O Yes	
Specify the host name a	nd port number for the Data Recovery Manager
Host name:	
Agent SSL port number:	
Timeout(Sec.):	30
	<back next=""> Cancel Help</back>

F-SECURE CORPORATION

WHITE PAPER

Select "No" to not connect to a remote Data Recovery Manager and click Next.

.1	Installation Wizard					×
	Network Configuration					
	Select the network port n	umbers CMS will u	use for:			
	SSL administration port:	8200				
	SSL agent port:	8100				
	SSL end-entity port:	443				
	Non-SSL end-entity port:	80	Enable:	•		
		<back< td=""><td>Next></td><td></td><td>Cancel</td><td>Help</td></back<>	Next>		Cancel	Help

Check the "Enable" box to enable "Non-SSL end-entity port." Click Next to continue.

© F-Secure Corporation

N Installation Wizard
Server Migration from Certificate Server 1.x - Step 1
Do you want to migrate your keys and certificates from a previous Netscape Certificate Server 1.x installation?
C Yes
€ No
<back cancel="" help<="" td=""></back>

Select "No" to not migrate keys and certificates from a previous installation and click *Next*.

N. Installation ₩izard		>
CA's serial number range -		
Specify the serial number serial number field blank m	range of the certificates that this CA issues. Leave the endineans unlimited.	ng
Starting serial number: 0×	1	
Ending serial number: 0×		
	<back next=""> Cancel Help</back>	

F-SECURE CORPORATION

WHITE PAPER

Enter a starting serial number of 1 and no ending serial number and click Next.

N Installation Wizard
CA Signing Certificate
Do you want to create a self-signed CA Certificate, or create a certificate signing request to submit to another CA?
Create self-signed CA Certificate
C Create subordinate CA Certificate Request
<back next=""> Cancel Help</back>

Select to "Create self-signed CA Certificate" and click Next.

C F-Secure Corporation

16

N Installation Wizard		×
_Key-Pair Information for Certifi	icate Manager CA Signing Certificate	
Select the token (cryptograp	hic device) for the key pair:	
Token: Internal 💌		
Initialize the selected token:		
Password:	******	
Password (again):	******	
Security officer password:		
Specify the key type and key	/ length:	
Key type: RSA 💌	-	
Key length: 1024 💌 l	bits	
Enter a value for the customiz	zed key length: bits	
	<back next=""> Cancel Help</back>	

Enter a password for the CA key-pair and select a key length of 1024 bits. Click Next.

N Installation Wizard
Message Digest Algorithm
Select hashing algorithm to use for computing signature on this certificate:
SHA1 💌
<back next=""> Cancel Help</back>

F-SECURE CORPORATION

Select a hashing algorithm of SHA1 and click Next.

Installation Wizard	
Subject Name for Certificate Ma	nager CA Signing Certificate
To modify the subject DN for th	
To mouny the subject on the	ie certificate.
Enter the values for the sub	ject DN components:
Common name (CN=):	Certificate Manager
Organizational unit (OU=):	Test Lab
Organization (O=):	FSecure
	Fsecure
Locality (L=):	
State (ST=):	
Country (C=):	FI
Selected DN:	CN=Certificate Manager, OU=Test Lab, O=FSecu re, C=FI
CN=Certificate Manager, C	=US

Enter the desired information for the CA Signing Certificate and click Next.

C F-Secure Corporation

18

4.	Installatio	n Wizar	d							×
	Validity Period for Certificate Manager CA Signing Certificate									
	Specify the validity period for the certificate:									
		YYYY	MM	DD	ΗH	mm	SS			
	Begin on:	2000	9	13	00	00	00			
	Expire on:	2002	9	13	00	00	00			
				<b< td=""><td>ack</td><td>N</td><td>ext></td><td>Cancel</td><td>Help</td><td></td></b<>	ack	N	ext>	Cancel	Help	

Select the validity period for the CA Signing Certificate. The default of 2 years should be sufficient. Click *Next*.

N Installation Wizard
Certificate Extensions for Certificate Manager CA Signing Certificate
Specify the certificate extensions:
☑ Basic constraints
CA
Certification path length:
Vetscape certificate type
SSL client SSL server SMIME SSL CA
Object-signing SMIME CA Object-signing CA
Authority key identifier
Subject key identifier
✓ Key usage
i noj dougo
Base64 of SEQUENCE of extensions
A .
Paste from Clipboard
<back next=""> Cancel Help</back>

F-SECURE CORPORATION

WHITE PAPER

Accept the default certificate extensions by clicking Next.



Click Next to generate and install the CA certificate.

20

N Installation Wizard
SSL Server Certificate
Do you want to sign this certificate with this CA's Signing Certificate, or do you want to create a certificate signing request to submit to another CA?
Sign SSL Certificate with my CA Signing Certificate
C Create request for submission to another CA
<back next=""> Cancel Help</back>

Select to "Sign SSL Certificate with my CA Signing Certificate" and click Next.

N Installation Wizard	×
Key-Pair Information for SSL Server Certificate	
Select the token (cryptographic device) for the key pair:	
Token: Internal	
Password:	
Password (again):	
Security officer password:	
Specify the key type and key length:	
Key type: RSA 💌	
Key length: 512 vits	
Enter a value for the customized key length:	
<back cancel="" he<="" td=""><td>elp</td></back>	elp

F-SECURE CORPORATION

Accept the default key-pair information for the SSL certificate by clicking Next.

Installation Wizard
Message Digest Algorithm
Select hashing algorithm to use for computing signature on this certificate:
SHA1 🔽
<back next=""> Cancel Help</back>

Select the hashing algorithm of SHA1 for the certificate and click Next.

C F-Secure Corporation

22

N Installation Wizard									
Subject Name for SSL Server C	ertificate								
To modify the subject DN for t	To modify the subject DN for the certificate:								
C Enter the values for the subject DN components:									
*Common name (CN=):	fsca.f-secure.com								
Organizational unit (OU=):	Test Lab								
Organization (O=):	FSecure								
Locality (L=):									
State (ST=):									
Country (C=):	FI								
Selected DN:	CN=fsca.f-secure.com, OU=Test Lab, O=FSecu e, C=FI								
C Enter the values for the sul	·								

Enter the desired information for the SSL Server Certificate. Note that the Common Name should be the fully qualified domain name of the server. Click *Next* to continue.

 Installatio	n Wizar	d							×
Validity Period for SSL Server Certificate									
Specify the	e validity	period 1	ior the c	ertificat	ie:				
YYYY MM DD HH mm SS									
Begin on:	2000	9	13	00	00	00			
Expire on:	2001	9	13	00	00	00			
			<b;< th=""><th>ack</th><th>N</th><th>ext></th><th>Cancel</th><th></th><th>Help</th></b;<>	ack	N	ext>	Cancel		Help

F-SECURE CORPORATION

WHITE PAPER

Enter the validity period for the SSL Server Certificate. Note that this must be less than the validity period for the CA Certificate. Select a one-year validity period and click *Next*.

N Installation Wizard
Certificate Extensions for SSL Server Certificate
Specify the certificate extensions:
Easic constraints
CA.
Certification path length:
✓ Netscape certificate type
SSL client SSL server SMIME SSL CA
Object-signing SMIME CA Object-signing CA
Authority key identifier
Subject key identifier
V Key usage
Base64 of SEQUENCE of extensions
▲
Paste from Clipboard
<back cancel="" help<="" td=""></back>

Accept the default certificate extensions by clicking Next.

C F-Secure Corporation

24

IN Installation Wizard	×
SSL Server Certificate Creation	1
The wizard has all the information required to generate the key pair and the corresponding certificate. Click Next to generate the certificate.	
<back cancel="" help<="" td=""><td></td></back>	

Click Next to generate the SSL certificate.

IN Installation Wizard
Create Single Sign-on Password
Single sign-on password is used to encrypt all the passwords that are required to start CMS.
Single sign-on password: *******
Single sign-on password (again): *******
Token for the Certificate Manager signing key and certificate:
Token name: Internal Key Storage Token
Token password: ******
Token for the Registration Manager signing key and certificate:
Token name:
Token password:
Token for the Data Recovery Manager transport key and certificate:
Token name:
Token password:
Token for the SSL server key and certificate:
Token name: Internal Key Storage Token
Token password: ******
<back next=""> Cancel Help</back>

F-SECURE CORPORATION

Enter a password to be used as the single sign-on password for CMS and click Next.



Click Done to complete the Installation Wizard.

As the final screen says, you should now connect to https://server:8100 and follow the instructions on the screen in order to get an agent certificate.

4.3 Configure SCEP Enrolment

Certificate Management System provides a menu-driven, interactive script to automate the configuration of the SCEP enrollment process. To use this script, follow the procedure below:

Create an SCEP Authorization file cepauth.txt in the C:\Netscape\Server4 directory. This file should contain a single line: "pwd: <password>" where <password> can be any authorizing password to be sent with the CEP request. For a more secure environment this file can include additional fields that can be used to identify authorized requests before processing them. For more information regarding this file see the CMS documentation.

Open a command prompt window on the CMS host system.

Change to the <root server> directory. (e.g. cd \netscape\server4)

Enter the following at the command prompt and press Enter:

install/perl.exe bin/cert/tools/cepconfig.pl

Press Enter a few times to get to the "Main Menu" screen.

C:\WINNT\System32\cmd.exe - install\perl.exe bin\cert\tools\cepconfig.pl	_ 🗆 ×
MAIN MENU	
LDAP Publishing for cert-fsca is currently: DISABLED.	
What would you like to do with cert-fsca	
 Configure a CEP service. Add another CEP service. Remove a CEP service. Enable LDAP publishing for cert-fsca (affects all CEP services). Disable LDAP publishing for cert-fsca (affects all CEP services). Restart the CMS server. Exit. 	
Your Choice (0-7): 4	

The first task is to enable LDAP publishing for the server. Enter "4".

C:\WINNT\System32\cmd.exe - install\perl.exe bin\cert\tools\cepconfig.pl	_ 🗆 🗵
LDAP PUBLISHING SETUP	
This instance of CMS has not been configured for LDAP publishing of certificates and CRLs yet. This will now be done for you.	
Found subject name of CA Certificate as: CN=Certificate Manager, OU=Test Lab, O=FSecure, C=FI,	
In order to configure LDAP publishing, some new schema needs to be added to your LDAP directory. For this, the directory manager password is required.	
At the prompt, enter the password for the 'CN=Directory Manager' user. THE PASSWORD WILL APPEAR IN THE CLEAR	
Password:	

When prompted enter the Directory Manager password and press Enter.

F-SECURE CORPORATION

WHITE PAPER

C:\WINNT\System32\cmd.exe - install\perl.exe bin\cert\tools\cepconfig.pl _ 🗆 × add objectclass: top person add cn: Certificate Manager add sn: **CA** Certificate adding new entry cn=Certificate Manager,O=FSecure modify complete Enabling LDAP publishing. Enter the CMS single-signon password: password LDAP publishing of certificates and CRLs is now ENABLED for cert-fsca. This means that each CEP service may now be configured for LDAP Publishing. If you want to enable LDAP Publishing for a CEP service, you must configure that service explicitly and enable LDAP Publishing for that service. You have made changes that will not become effective until the CMS server has been restarted. Do you want to restart the server now? Restart (y/n)? n

When prompted enter the CMS single sing-on password and press Enter.

Enter "n" to not restart the server at this time. This will be done once the configuration is complete.

You should now be back to the Main Menu. Enter "1" to configure a CEP service.



Enter "1" to configure the default CEP service.

F-SECURE CORPORATION

CONFIGURE CEP SERVICE CONFIGURE CEP SERVICE Current Configuration: Service Name......Default CEP Service Service URL.......Default CEP Service Service URL......Disabled. Autoenrollment......Disabled. What would you like to do with 'Default CEP Service'? 1) Rename this CEP service. 5) Enable autoenrollment. 2) Change the service URL. 6) Disable autoenrollment. 3) Enable LDAP publishing. 7) Configure autoenrollment 4) Disable LDAP publishing. Ø) Return to main menu. Your Choice (Ø-8): 3 LDAP publishing of certificates and CRLs is now enabled for Default CEP Service. You have made changes that will not become effective until the CMS server has been restarted. Do you want to restart the server now? Restart (y/n)? n_

Enter "3" to enable LDAP publishing for the CEP service.

When prompted, enter "n" to not restart the CMS server.

Back at the Configure CEP Service menu enter "5" to enable autoenrollment.

Enter the path to the password file that you created earlier (e.g. c:\netscape\server4\cepauth.txt) and press Enter.

WHITE PAPER

Again, enter "n" to not restart the CMS server and press Enter to return to the Configure CEP Service menu.

Enter "7" to configure autoenrollment.

C:\WINNT\System32\cmd.exe - install\perl.exe bin\cert\tools\cepconfig.pl	- 🗆 ×
CONFIGURE AUTOENROLL	
Current Configuration:	
Service NameDefault CEP Service Service URL/cgi-bin/pkiclient.exe LDAP publishingEnabled. AutoenrollmentEnabled. Authentication filec:/Netscape/Server4/cepauth.txt Key AttributesIPAddress Auth Attributespwd Defer on failurefalse	
What autoenroll settings would you like to change? 1) Change authentication file location. 2) Add key attributes. (currently: IPAddress) 3) Remove key attributes. 4) Change defer on failure setting. (currently: false) Ø) Return to previous menu.	
Your Choice (0-5): 3_	

Enter "3" to remove key attributes.

C:\WINNT\System32\cmd.exe - install\perl.exe bin\cert\tools\cepconfig.pl	_ 🗆 ×
 Change authentication file location. Add key attributes. (currently: IPAddress) Remove key attributes. Change defer on failure setting. (currently: false) Return to previous menu. 	
Your Choice (0-5): 3 Current Key Attributes: IPAddress Which key attribute do you want to remove?	
0) Done removing. 1) IPAddress	
Your Choice (0-1): 1 Current Key Attributes: IPAddress	
Which key attribute do you want to remove?	
0) Done removing.	
Your Choice (0): 0	

Enter "1" to remove the IPAddress attribute.

Enter "0" to return to the Configure CEP Service Menu.

F-SECURE CORPORATION

Enter "0" to return to the Main Menu.

Enter "6" to restart the CMS Server.

Netscape Certificate Se	rver
Enter the password for	"Single Sign On for CMS instance fsca":
2	******
	Cancel

Enter the CMS Single Sign-On password and click OK.

Enter "0" to exit the script.

5 Integration with F-Secure VPN+

5.1 Add CA Certificate as Trusted Root

5.1.1 Export CA Certificate

Launch a web browser and go to https://<cms server>:8100.

Click on the "Certificate Manager Agent Services" link.

Click on the "List Certificates" link.

Click the *Find* button.

Click on the Details button of the certificate with serial number 0x00000001

Scroll down and copy the Base 64 encoded certificate details to an empty text file including the BEGIN CERTIFICATE and END CERTIFICATE lines.

Save the text file to a temporary location as cms_ca.pem (e.g. c:\temp\cms_ca.pem)

5.1.2 Import CA Certificate as Trusted Root

On the F-Secure Policy Manager Console computer, start F-Secure Administrator (Start – Programs – F-Secure Policy Manager Console.)



In the F-Secure Administrator (FSA) select the policy domain or host that you wish to enroll via SCEP.

Browse to F-Secure/F-Secure Management Agent/Settings/Certificate Handling/Certificates/Trusted item in the Properties pane.

Click on the *Add* button and browse to find the CA root certificate file that you created when exporting the CA certificate in the section above. Click *Open*.

Enter a descriptive comment (e.g. Netscape CA).

4.1 Configure Certificate Handling

4.1.1 Enable SCEP Enrollment

F-Secure VPN+ hosts can enroll for host certificates using the Simple Certificate Enrollment Protocol (SCEP.) An example of the policy settings that need to be configured is shown in the image below. The image is a snapshot of the settings under the F-Secure/F-Secure Management Agent/Settings/Certificate Handling section of the policy.



4.1.2 Enable CRL Retrieval

F-Secure VPN+ supports Certificate Revocation List (CRL) retrieval. If certificates are revoked from the CA, the serial numbers of the revoked certificates are stored in a CRL in the LDAP directory.

As IPSec connections are established between hosts, the host will check the CRL of the issuing CA to ensure that the certificate has not been revoked. This CRL is cached locally on the host for future use. A new CRL is fetched from the LDAP directory when the old CRL expires. The CRL Trust Time policy setting in FSA can be used to define how often to try to fetch a new CRL even if the host has a valid CRL available. Normally a CA system issues CRLs periodically, but they may also issue a new CRL right after a certificate has been revoked. This CRL Trust Time setting can be used to assure that the revocation information is transferred to the host faster than the normal CRL update time.

An example of the policy settings that need to be configured to enable CRL retrieval is shown in the image below. The image is a snapshot of the settings under the F-Secure/F-Secure Management Agent/Settings/Certificate Handling section of the policy.



4.2 Create Connection Template

Once the certificates have been installed on the required hosts and/or gateways according to the steps above, you are ready to create an IPSec connection. Again, these can either be centrally managed using F-Secure Administrator (recommended) or set up manually

F-SECURE CORPORATION

on each client. For the purposes of this document, the creation of a simple host-togateway IPSec connection will be demonstrated below.

In FSA, browse to the F-Secure/F-Secure VPN+/Settings/Connections item.

New Connection Te	emplate Wizard	×
F-SECURE'	This wizard will help you to add a new rule or connection template. The new template is numbered as 2.	
	C Distributed Firewall Rule	
	C User Definable Connections and Rules	
	<u>C</u> ancel ≤ <u>B</u> ack <u>N</u> ext > Emit	sh

Click on the Add button to add a new connection.

Select "VPN+ Connection" and click Next.

C F-Secure Corporation

34

New VPN+ Connec	tion Template Wizard	×
F-SECURE"	Please select what kind of connection template to create. "Host to Host" template is used for connecting multiple VPN+ enabled hosts, e.g. F-Secure VPN+ Client(s) connecting to F-Secure VPN+ Server. "Gateway'to Gateway'template allows you to connect remote LANs with F-Secure Gateways. "Host to Gateway' template is used for remote access connections, e.g. Dial-up Clients connecting to a LAN through F-Secure Enterprise Gateway.	
	C Host to Host	
	 Gateway to Gateway ← Host to Gateway 	
	<u>Cancel</u> < <u>Back</u> <u>Next</u> > <u>Einish</u>	

Select "Host to Gateway" and click Next.

Host to Host Conne	ction Template Wizard	×
F-SECURE D	Please select the connection type. Select "IPSec" for secured connections, "Bypass" for cleartext connections, and "Discard" to disallow traffic between the endpoints.	
	Connection Type	
	C Bygass	
	C <u>D</u> iscard	
	Cancel < Back Next > Elmish	

Select a connection type of "IPSec" and click Next.

Host to Gateway Co	onnection Template Wizard
F-SECURE"	Specify the host endpoint. You can select any policy domain or host to be the endpoint. Alternatively you can specify the host endpoint as IP address or DNS name. IP address can be a host IP address (e.g. 192.168.100.100), a network (e.g. 192.168.100.0/24), or a range of IP addresses (e.g. 192.18.100.1+192.168.100.10). If you want to use smartcard-based user authentication for remote access, please fill in the organizational information of smartcard users. Empty fields are treated as wildcards. With smartcard authentication it is recommended to use a policy domain as host endpoint.
	Smartcard authentication Allowed User Certificates Country: Don't care Organization: Organization Unit Organization Unit Common Name: Additional Fields: Connection Endpoint Host Endpoint dfsmurfli
	<u>C</u> ancel <u>Back</u> <u>N</u> ext > <u>Finish</u>

Select the desired host endpoint for the host-to-gateway connection. This endpoint can be a single host or a security domain (group of hosts.) On this screen it is also possible to configure the connection to use smart card authentication. If this is desired, check the "Smartcard authentication" checkbox and fill in the identifying fields for the allowed smart cards. When all required settings are filled, click *Next*.

Note: If "Smartcard authentication" is checked but no fields are filled, you must enter sc[] in the "Additional Fields" box for the connection to work.

Host to Host Conne	ction Template Wizard	×
F-SECURE"	Select IKE properties required	for the connection.
- And -	<u>M</u> ode:	Main
	Proposa <u>l</u> list:	Use Default from IKE Settings
	<u>P</u> FS:	None
7	<u>G</u> roup:	Oakley group 1
	IKE SA Life <u>t</u> ime (KBytes):	Use Default from IKE Settings
	IKE <u>S</u> A Lifetime (seconds):	Use Default from IKE Settings
	Pre-shared <u>k</u> ey:	
	<u>C</u> ancel	< <u>B</u> ack <u>N</u> ext >inish

Leave the IKE settings at the default values and click Next.



Leave the IPSec settings at the default values and click Next.

Host to Host Conne	ection Template Wizard X	
Specify which services in which direction a filters. If it is to filter a service which requires several service entries, like WINS(1) and WINS(2), please remember to add all of them.		
	Service Endpoint1 / Local ID Direction Endpoint2 / Remote ID	
	✓ Include all traffic	
	Add Edit Remove RemoveAll	
	Cancel < Back Next > Enish	

Leave the traffic filtering settings at the default of "Include all traffic" and click Next.

Note: Configured traffic filters are only used if F-Secure Distributed Firewall is also installed on the client computers.

Host to Host Connection Template Wizard			
F-SECURE"	Many different flags can be specified for the endpoints of this rule. Flags are comma-separated and parameters are specified after a colon.		
	Flags		
	Endpoint <u>1</u> flags:		
	Endpoint <u>2</u> flags:		
	<u>Cancel</u> < <u>Back</u> <u>Next</u> > <u>Finish</u>		

Leave the endpoint flags empty and click Next.

```
F-SECURE CORPORATION
```

Host to Host Connection Template Wizard				
F-SECURE"		connection template displayed below. You can edit (Cancel) this connection template.		
-	Endpoint1:	fspki		
	Endpoint2:	fsdemo05		
	Connection Type:	IPSec		
	IKE Mode:	Main		
	IKE Proposal:	Use Default from IKE Settings		
The second second	IKE PFS:	None		
	IKE SA Lifetime (KBytes):	Use Default from IKE Settings		
	IKE SA Lifetime (seconds):	Use Default from IKE Settings		
	Pre-shared key:			
	IPSec Pronosal:	Lise Default from IKE Settings 🛛 🔳		
	Comment: Test Connection			
	Commente prest Connection			
-	Cancel	< Back Next > Finish		

Add a descriptive comment if desired and click Finish.

Distribute the updated policy by selecting Distribute from the File menu.

Once the VPN+ hosts have received the updated policy, test the connection you just created by "pinging" from the VPN+ client to a host on the other side of the gateway.

5.2 Known Issues

No known issues at this time.

C F-Secure Corporation